WHAT IS CLAIMED

1. A method of identifying data in a network exploit, comprising:

receiving a packet by an intrusion prevention system maintained by a node of a network, the intrusion prevention system bound to a media access control driver and a protocol driver;

invoking a signature analysis algorithm by the intrusion prevention system; and

comparing the packet by the intrusion prevention system with a first rule set comprising a rule logically defining a packet signature.

2. The method according to claim 1, wherein receiving a packet by an intrusion prevention system further comprises receiving a packet originating from the node.

3. The method according to claim 1, wherein receiving a packet by an intrusion prevention system further comprises receiving a packet originating from a source external to the node, the packet addressed to the node.

4. The method according to claim 1, further comprising discarding the packet upon determination that a signature of the packet corresponds to the rule.

5. The method according to claim 1, wherein comparing the packet by an intrusion prevention system with a first rule set further comprises comparing the packet by the intrusion prevention system with a second rule set upon determination that a signature of the packet does not correspond to a rule of the first rule set.

6. The method according to claim 1, wherein comparing the packet by the intrusion prevention system with a first rule set further comprises comparing the packet by the intrusion prevention system with a rule set comprising a plurality of

rules each respectively comprising machine-readable code logically defining a packet signature.

7. A node of a network maintaining an instance of an intrusion prevention system for identifying data in a network exploit, the node comprising:

a central processing unit;

a memory module for storing data in machine-readable format for retrieval and execution by the central processing unit; and

an operating system comprising a network stack comprising a protocol driver, a media access control driver and an instance of the intrusion prevention system bound to the protocol driver and the media access control driver, the intrusion prevention system comprising an associative process engine and an input/output control layer, the input/output control layer operable to receive a signature file generated from a network exploit rule comprising an operand, an operator and a mask, the input/output control layer operable to pass the signature file to the associative process engine, the associative process engine operable to analyze a data packet with the signature file and assign a logical value to the signature file dependent upon a result from the analysis.

8. The node according to claim 7, wherein the exploit rule further comprises a composite of a plurality of rules, each rule comprising an operand, an operator and a mask and having a logical value, each of the plurality of rules being logically connected with at least one of the other plurality of rules by a non-bitwise boolean operator, the logical value of the signature file dependent on the logical value of each of the plurality of rules.

9. The node according to claim 7, wherein the operand comprises network frame data, the operator comprises a bitwise operation, and the mask comprises an operator mask.

10. The node according to claim 7, wherein the network control layer is operable to receive a plurality of signature files each respectively generated from a network exploit rule.

11. The node according to claim 10, wherein a parametric association is assigned to a subset of the plurality of signature files, the associative process engine operable to determine a parametric value of the packet and to analyze the packet with the subset of the signature files when the parametric association of the signature files coincide with the parametric value of the packet.

12. The node according to claim 11, wherein the parametric value of the packet is obtained from link-layer header information of the packet.

13. The node according to claim 11, wherein a plurality of parametric associations are respectively assigned to a plurality of subsets of signature files.

14. The node according to claim 11, wherein the parametric association is one of a plurality of parametric associations, each of the plurality of parametric associations comprising a common subset of signature files, each signature file of the common subset respectively analyzed by the associative process engine against the network packet prior to analyzation of any other signature files of any other subsets of signature files.

15. The node according to claim 10, further comprising a table maintained in the memory module, the table comprising a plurality of indices each respectively indexing a subset of the plurality of subsets of signature files.

16. The node according to claim 7, wherein the intrusion prevention system further comprises an intrusion event manager, the associative process engine operable to communicate that the analysis of the packet indicates a correspondence with the signature file, the intrusion event manager operable to generate an alert that is

transmitted from the node to at least one of a management node in a network and an event database maintained by the node.

17. A computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of:

reading a data packet;

selecting a set of a plurality of signature files from a plurality of sets of signature files, each respective signature file of the plurality of sets of signature files generated from a respective rule of at least one rule set comprised of a plurality of rules; and

comparing the data packet with at least one signature file of the selected set.

18. The computer readable medium according to claim 17, further comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of determining whether a correspondence between a signature of the data packet and the at least one signature files exists.

19. The computer readable medium according to claim 17, further comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of comparing the data packet with each signature file of the selected set of the plurality of signature files.

20. The computer readable medium according to claim 19, further comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of:

upon determining that no correspondence exists between the signature of the data packet and the signature files of the selected set of the plurality of signature files, selecting a second set of signature files from the plurality of sets of signature files; and

comparing the signature of the data packet to at least one signature file of the second set of signature files.